In the Claims:

1. (Previously Presented) A method for securing circulation of an encrypted digital document to be reproduced with a document reader, the method comprising:

providing a user with a storage device storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated with the storage device;

transmitting to a server over the digital data transmission network from the storage device to the server upon connection of the storage device to the server by a terminal connected to the digital data transmission network and to the storage device

information identifying the digital document to be reproduced, and

the information list and the identification information of the storage device;

identifying from the server the storage device on the basis of the information identification of the storage device transmitted to the server;

determining possible fraudulent use of the storage device based upon the information list that is transmitted to the server, the server comparing the identification information in the information list with an authorized or fraudulent reader list for determining fraudulent use of the storage device;

if the storage device is not being fraudulently used, then transmitting over the digital data transmission network from the server to the computer terminal a decryption key specific to the digital document to be reproduced, with the decryption key being stored in the storage device;

decrypting the digital document using the stored decryption key by the document reader connected to the storage device; and

reproducing the digital document decrypted by the document reader.

2. (Previously Presented) The method according to Claim 1, wherein the decryption key is transmitted from the storage device to the document reader only if the document reader is authorized.

3. (Previously Presented) The method according to Claim 1, wherein if the storage device is being fraudulently used, then the decryption key is not transmitted from the server to the storage device; and further comprising deactivating the storage device by the server for prohibiting further use of the storage device.

4. (Previously Presented) The method according to Claim 1, wherein the information list also identifies unauthorized document readers; and wherein fraudulent use of the storage device is also determined if the identification information associated with the document reader is on the

information list.

5. (Previously Presented) The method according to Claim 4, wherein the server builds from the identification information of the storage device and from the information list received from the storage device a table containing, for each identified document reader, a number of different storage devices used with the document reader; and further comprising:

determining that a particular document reader is unauthorized if the corresponding number of different storage devices used with this particular document reader exceeds a threshold; and

inserting the identification information of the document reader determined to be unauthorized into an unauthorized document reader list.

6. (Previously Presented) The method according to Claim 1, wherein if the storage device is being fraudulently used, then the decryption key is not transmitted over the digital data transmission network from the server to the storage device.

7. (Previously Presented) The method according to Claim 1, wherein if the storage device is being fraudulently used, then the server deactivates the storage device over the digital data transmission network for prohibiting any further use of the storage device for reproducing a digital document.

8. (Previously Presented) The method according to Claim 1, wherein the decryption key specific to the digital document being reproduced is stored in the storage device in association with the information identifying the digital document to be reproduced; and wherein the document reader transmits to the storage device the information identifying the digital document that has been transmitted to it for reproducing, and then receives from the storage device the decryption key associated with the information identifying the digital document for decrypting the digital document.

9. (Previously Presented) A method for securing circulation of an encrypted digital document to be reproduced with a document reader, the method comprising:

providing a user with a smart card storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers operated with the smart card;

transmitting to a server over the Internet from the smart card to the server upon connection of the smart card to the server by a computer terminal connected to the Internet and to the smart card

information identifying the digital document to be reproduced, and

the information list and the identification information of the smart card;

identifying from the server the smart card on the basis of the information identification of the smart card transmitted to the server;

determining possible fraudulent use of the smart card based upon the information list that is transmitted to the server, the server comparing the identification information in the information list with an authorized or fraudulent document reader list for determining fraudulent use of the smart card;

if the smart card is not being fraudulently used, then transmitting over the Internet from the server to the computer terminal a decryption key specific to the digital document to be reproduced, with the decryption key being stored in the smart card;

decrypting the digital document using the stored decryption key by the document reader connected to the smart card; and

reproducing the digital document decrypted by the document reader.

10. (Previously Presented) The method according to Claim 9, wherein the decryption key is transmitted from the smart card to the document reader only if the document reader is authorized.

11. (Previously Presented) The method according to Claim 9, wherein if the smart card is being fraudulently used, then the decryption key is not transmitted from the server to the smart card; and further comprising deactivating the smart card by

the server for prohibiting further use of the smart card.

12. (Previously Presented) The method according to Claim 9, wherein the information list also identifies unauthorized document readers; and wherein fraudulent use of the smart card is also determined if the identification information associated with the document reader is on the information list.

13. (Previously Presented) The method according to Claim 12, wherein the server builds from the identification information of the smart card and from the information list received from the smart card a table containing, for each identified document reader, a number of different smart cards used with the document reader; and further comprising:

determining that a particular document reader is unauthorized if the corresponding number of different smart cards used with this particular document reader exceeds a threshold; and

inserting the identification information of the document reader determined to be unauthorized into an unauthorized document reader list.

14. (Previously Presented) The method according to Claim 9, wherein if the smart card is being fraudulently used, then the decryption key is not transmitted over the Internet from the server to the computer terminal.

15. (Previously Presented) The method according to Claim 9, wherein if the smart card is being fraudulently used, then the server deactivates the smart card over the Internet for prohibiting any further use of the smart card for reproducing a digital document.

16. (Previously Presented) The method according to Claim 9, wherein the decryption key specific to the digital document being reproduced is stored in the smart card in association with the information identifying the digital document to be reproduced; and wherein the document reader transmits to the smart card the information identifying the digital document that has been transmitted to it for reproducing, and then receives from the smart card the decryption key associated with the information identifying the digital document for decrypting the digital document.

17. (Previously Presented) A system for securing circulation of an encrypted digital document to be reproduced with a document reader, the system comprising:

a storage device storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated with said storage device;

a server connected to a digital data transmission network;

at least one terminal connected to the digital data transmission network and interfacing with said storage device for

transmitting to said server the information identifying said storage device along with information identifying the digital document to be reproduced;

receiving from said server a specific decryption key for decrypting the digital document to be reproduced, with the decryption key being stored in said storage device, and

transmitting to said server the information list which is transmitted from said storage device to said server upon connection of said storage device to said server; and

said document reader for interfacing with said storage device and for reproducing the encrypted digital document, said document reader receiving from said storage device the decryption key for the digital document to be decrypted and reproduced and comprising

a memory for storing the digital document to be reproduced and the decrypted key,

a decoder for decrypting the digital document to be reproduced based upon the stored decryption key; and

said server determining fraudulent use of said storage device based upon the identification information in the information list, said server comparing the identification information in the information list with an authorized or

fraudulent document reader list for determining fraudulent use of said storage device.

18. (Previously Presented) The system according to Claim 17, wherein the decryption key is transmitted from said storage device to said document reader only if said document reader is authorized.

19. (Previously Presented) The system according to Claim 17, wherein if said storage device is being fraudulently used, then the decryption key is not transmitted from said server to said storage device; and wherein said server deactivates said storage device for prohibiting further use.

20. (Previously Presented) The system according to Claim 17, wherein the information list also identifies unauthorized document readers; and wherein fraudulent use of said storage device is also determined if the identification information associated with said document reader is on the information list.

21. (Previously Presented) The system according to Claim 20, wherein said server builds from the identification information of said storage device and from the information list received from said storage device a table containing, for each identified document reader, a number of different storage devices used with said document reader, said server

determining that a particular document reader is unauthorized if the corresponding number of different storage devices used with this document reader exceeds a threshold; and

inserting the identification information of said document reader determined to be unauthorized into an unauthorized document reader list.

22. (Previously Presented) The system according to Claim 17, wherein if said storage device is being fraudulently used, then the decryption key is not transmitted over the digital data transmission network from said server to said storage device.

23. (Previously Presented) The system according to Claim 17, wherein if said storage device is being fraudulently used, then said server deactivates said storage device over the digital data transmission network for prohibiting any further use of said storage device for reproducing a digital document.

24. (Previously Presented) The system according to Claim 17, wherein the decryption key specific to the digital document being reproduced is stored in said storage device in association with the information identifying the digital document to be reproduced; and wherein said document reader transmits to said storage device the information identifying the digital document that has been transmitted to it for reproducing, and then receives from said storage device the decryption key

associated with the information identifying the digital document for decrypting the digital document.

25. (Previously Presented) A system for securing circulation of an encrypted digital document to be reproduced with a document reader, the system comprising:

a smart card storing identification information identifying the smart card and for storing an identification information list comprising identification information identifying recent document readers previously operated with said smart card;

a server connected to the Internet;

at least one computer terminal connected to the Internet and interfacing with said smart card for

transmitting to said server the information identifying said smart card along with information identifying the digital document to be reproduced,

receiving from said server a specific decryption key for decrypting the digital document to be reproduced, with the decryption key being stored in said smart card, and

transmitting to said server the information list which is transmitted from said smart card to said server upon connection of said smart card to said server;

said document reader for interfacing with said smart card and for reproducing the encrypted digital document, said document reader receiving from said smart card the

decryption key for the digital document to be decrypted and reproduced and comprising

a decoder for decrypting the digital document to be reproduced based upon the stored decryption key; and

said server determining fraudulent use of said smart card based upon the identification information in the information list received from said smart card.

26. (Previously Presented) The system according to Claim 25, wherein said smart card comprises a secure memory area for storing the identification information thereof.

27. (Previously Presented) The system according to Claim 25, wherein the decryption key is transmitted from said smart card to said document reader only if said document reader is authorized.

28. (Previously Presented) The system according to Claim 25, wherein said server is configured to not transmit the decryption key to said smart card and to deactivate said smart card for prohibiting further use thereof if said smart card is being fraudulently used.

Claim 29 (Cancelled).

30. (Previously Presented) The system according to Claim 25, wherein the information list also identifies

unauthorized document readers; and wherein fraudulent use of the smart card is also determined if the identification information of said document reader is on the information list.

31. (Previously Presented) The system according to Claim 30, wherein said server builds from the identification information of said smart card and from the information list received from said smart card a table containing, for each identified document reader, a number of different smart cards used with said document reader, said server

determining that a particular document reader is unauthorized if the corresponding number of different smart cards used with this particular document reader exceeds a threshold; and

inserting the identification information of said document reader determined to be unauthorized into an unauthorized document reader list.

32. (Previously Presented) The system according to Claim 25, wherein if said smart card is being fraudulently used, then the decryption key is not transmitted over the Internet from said server to said smart card.

33. (Previously Presented) The system according to Claim 25, wherein if said smart card is being fraudulently used, then said server deactivates said smart card over the Internet for prohibiting any further use of said smart card for reproducing a digital document.

34. (Previously Presented) The system according to Claim 25, wherein the decryption key specific to the digital document being reproduced is stored in said smart card in association with the information identifying the digital document to be reproduced; and wherein said document reader transmits to said smart card the information identifying the digital document that has been transmitted to it for reproducing, and then receives from said smart card the decryption key associated with the information identifying the digital document for decrypting the digital document.